Do cryptocurrencies need to be regulated?

Sadegh Bamohabbat Chafjiri

September 19, 2020

1 Abstract

Allocating telecommunications frequencies is a governance issue for any purpose of the use by telecommunication services. All cryptocurrencies; transactions are performed on the telecommunication bands. Therefore cryptocurrency can not be free from governmental regulations while it has this potential to make monopoly in the frequency allocations. This article comes up with this idea that how an architecture can be designed in the network layer to use the cryptocurrency as the global currency to meet local government regulations. I explain why the absence of the governance plan challenges the cryptocurrencies future and its digital economy and I particularly evaluate lack of governance model on the VOIP service. I discuss that the current business model of cryptocurrencies work inside the particular territory of country or financial system and cryptocurrencies require to have transparent governance plan for other counties' financial systems. I discuss that cryptocurrency's market is vulnerable against political factors and rules that govern different territories. I describe why we need to consider cryptocurrency not as the currency but also as the service when vendors provide their own cryptocurrencies in the application layer of the OSI model. Finally, I conclude this issue can be resolved by combination of cryptocurrencies as the service in the application layer and regulated cryptocurrencies as in the network layers.

2 introduction

In [A], authors recommended the decentralized keystore based on the blockchain to hold the Users' public keys. Its method eliminates the role of (CA) Certificate Authority in the user authentication of VOIP service by retrieving the public key from blockchain. The system architecture uses the Ethereum wallet and Light Ethereum Subprotocol (LES) features. According to [B], LES enables VOIP service to fetch other parts of the blockchain on-demand to provide better functionality without taking part in the mining or consensus process. Recommended model is a primary solution which technically works as long as the cryptocurrency is used for the particular territory. However, there are few points of concern about governance model of this cryptocurrency which I discuss in section 3.

3 The problem

I believe the blockchain network in this article and other similar research in blockchain suffer from lack of governance model. They should have a clear governance plan to grow in different country. In the governance model, it should explain what the company maps out as the strategy for the node selections in blockchain. It might vary country by country to meet political requirements. Political requirements sometimes urge technical requirements not seen at first glance like what Britain's Financial Conduct Authority forces for anti-money laundering [C]. Another example showing the power of political factors would be the Huawei's case of sanction in the US [D]. Huawei impacted by US regulations only because one of the supplychain block (semi-conductors) is located inside the US borders. Therefore, designers of blockchain need to consider the political factors as the influencing terms in their designs to reduce their effects on the decentralized network. Moreover, political factors impact the business model too. As long as the blockchain network is located inside the country's territory, designers may ignore the political factors internationally. However, it is not true for capital growth overseas. In other words, the governance model of cryptocurrency will be involved in other factors to keep the supplychain up. Therefore, blockchain network might eliminate the role of intermediaries like financial firms or banks in the centralized management system, however it is not supposed to eliminate the role of centralized government reserving the right of indigenous people in the particular territory.

4 Available solutions

Interestingly, the blockchain network possesses the flexible model to offer the similar financial terms in the governance model like cryptotax, cryptotariff, cryptocharge, cryptofinance, cryptoloan, cryptoinvestment, cryptobank and etc. In other words, blockchain network should go forward to standardize the framework of cryptocurrency per service (HTTP, UDP and etc) not per network or per device. Here is an example. Imagine the VOIP service provider A has its own chain of devices to guarantee the higher level of privacy. Is there any guarantee that company B providing the same VOIP service would not use independent miners already employed in VOIP service provider A. what will happen for privacy of A if B want to use the mining power of A. What will happen for owners of coins when the company goes bankrupt and there is no domain to keep wallets? and how customer is able to use the coins as the assets for other VOIP services in case the company A became out of competition. Nokia is a good example of companies became out of competition in the smart phone generation and its supply chain network could not continue. Imagine Nokia had its own blockchain and coin. In that assumption, how a customer could complete its service request through wallets embedded per device on Nokia infrastructure while the confirming nodes became out of service. Who is the reference of network response in the failure scenario. It urges a public reference for response for services. So, It determines the importance of the blockchain consistency and bolds the coin as a public service in the network layer rather than private service in the application layer.

5 Recommended solution

What is solution? I would discuss it for specific service which is Voice over IP. Most of countries agree on the telecommunication frameworks and standards. For example, UDP framework can be the basis of blockchain for RTP or streaming services including VOIP. UDP framework can have its own blockchain and its own coin independent of the type of streaming service uses in the application layer. Blockchain network servicing in application layer can design their own schemes and can define their own coin as a function of UDP coin for the amount of value added to customer or the level of integrity ensures for authentication purposes. Another problem which bold the crucial role of basic coins in network layer is that each service needs a network capacity to support its coins technically. All of confirmation per node increase the demands and can impact on the capacity of network. Private sectors might monopolize channels in the competitive market to keep their coins value. Some nodes might be involved in counterfeiting the coins by monopolizing of nodes away from the inspector's eyes. It means designers of cryptocurrency's infrastructure require to define inspector nodes across the blockchain network too. The best candidates are able to regulate this area would be global telecommunication authorities (ITU, IETF). In this model, all authorities such as ITU can supervise and regulate different application for their violations.

6 Next step and other points of views:

Different blockchain might have different cryptocurrency derived from the basic cryptocurrency in the network layer. Basic coins are available on network layer and not available on application layer. For example, SWIFT or VISA are platforms to transfer money from one country to another country. They follow countries' political factors too but different banks only need to meet SWIFT's or VISA's terms and conditions. If a cryptocurrency like Ripple wants to provide the similar but the decentralized service, why SWIFT or VISA could not do that on their available blockchain nodes with less complexity? As you know SWIFT or VISA already have the opportunity to employ the cryptocurrency as the service for world-wide customers. Both vendors already have this position and publicity in the world-wide transactions to eliminate the role of banks as the intermediaries. According to [5], "there is no reason SWIFT couldn't develop their own blockchain technology and use their already established relationships to roll it out faster than Ripple can grow.” Therefore, It has crucial to have a good vision for cryptocurrency usage in the decentralized environment.

7 Conclusion

To conclude, a decentralized and worldwide service needs decentralized governance model as well as decentralized infrastructure. I feel it would be interesting topic for more discussion particularly from IETF perspective.

8 References

A Elie Kfoury, David Khoury, Secure End-to-End VoIP System based on Ethereum Blockchain, Retrieved from http://www.jocm.us/uploadfile/2018/0817/20180817033654165.pdf

B Rjl493456442, Fjl, and Zsfelfoldi. (May, 2020), Light Ethereum Subprotocol (LES), Retrieved from https://github.com/ethereum/devp2p/blob/master/caps/les.md

C Ana Alexander. (Jan, 2020) UK Financial Watchdog FCA Now Supervises AML/CTF Compliance of Crypto Businesses Retrieved from https://cointelegraph.com/news/uk-financial-watchdog-fca-now-supervises-aml-ctf-compliance-of-crypto-businesses

D Originally published by Coin and Crypto. (Jan, 2018), 5 alarming reasons Ripple might not be what you think, Retrieved from https://hackernoon.com/4-alarming-reasons-ripple-might-not-be-what-you-think-9debc3c86985